WHAT IS CLAIMED IS:

1. A method for operating a computer system comprising a plurality of computers connected by a network, said computer system including an administrative computer, A, and a client computer, C, said method comprising the steps of:

providing a badge secured to one of said authorized individuals, said badge having a data processing system having a non-volatile memory, a volatile memory, a transceiver for sending and receiving signals utilized by said badge, and an attachment sensor for detecting the removal of said badge from that individual, said attachment sensor causing information stored in said volatile memory to be rendered unreadable when said attachment sensor detects said removal;

providing A with a transceiver for communicating with one of said badges and an identity verification system for authenticating the identity of that individual; and

causing A to load information in said volatile memory of said badge attached to that individual in response to said identity verification system authenticating that individual, said information specifying the level of access to said computer system to which that authorized individual is entitled.

2. The method of Claim 1 wherein said step of causing A to load information comprises the steps of:

establishing a secure communication channel between A and that badge by encrypting signals sent and received by said transceivers in A and that badge; and

sending said information on said secure communication channel.

3. The method of Claim 1 wherein said identity verification system compares the retina of that individual with data derived from a previous measurement on that individual's retina.

4. The method of Claim 1 wherein said identity verification system compares a finger print of that individual with data derived from a previous measurement on that individual's finger print.

5. The method of Claim 1 wherein said identity verification system compares the voice of that individual with data derived from a previous measurement on that individual's voice.

6. The method of Claim 1 wherein said identity verification system compares answers to queries posted to that individual with data previously provided by that individual.

7. The method of Claim 1 further comprising the steps of:

providing C with a transceiver for communicating with said badge attached to that individual;

causing C to verify the authenticity of that badge by receiving data derived from the data stored in said volatile memory of that badge by A;

causing C to provide that individual with access to said network, said access depending on said data stored in said badge.

8. The method of Claim 7 wherein C periodically verifies the presence of that individual by sending to and receiving signals from that badge.

9. The method of Claim 8 wherein C utilizes a first secure code to exchange data with that badge during said verification step.

10. The method of Claim 9 wherein C utilizes a second secure code to verify the presence of that individual, said second secure code requiring less computational resources than said first secure code.

11. The method of Claim 10 wherein said second secure code depends on said first secure code and changes each time C verifies the presence of that individual.

12. The method of Claim 1 wherein said information loaded by A into that badge includes a code that is periodically changed.